SOCIAL MEDIA ANALYTICS: A NEW APPROACH FOR CYBERSPACE ENABLED UNDERSTANDING OF OPERATIONAL ENVIRONMENTS

A Monograph

by

MAJ Sean P. Lyons
United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2013-02

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
12-05-2013	SAMS MMAS Monograph	JAN 2013 – DEC 2013

4. TITLE AND SUBTITLE

Social Media Analytics: A New Approach for Cyberspace Enabled Understanding of Operational Environments

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Sean Lyons

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Current Army doctrine emphasizes network defense and offensive strike capabilities for cyberspace activities, but does not expound on focusing advanced analytical tools for increasing shared understanding of the cyberspace information environment; then using that understanding to solve problems existing in a dual cyberspace-land domain. Global interconnectedness and the speed of change demand a new approach. This monograph explores Social Media Analytics (SMA) as a capability for providing Army commanders and staffs with cyberspace tools for generating human centric understanding. The research addresses SMA applied to a gap in contemporary Joint and Army doctrine, and evaluates SMA as an approach to bridging that gap. The topic is pertinent for military practitioners because SMA, and user generated content in cyberspace, present opportunities to increase operational tempo and the adaptability of Army operational and tactical level echelons by providing near-real time understanding through trending. The Army echelons directed to physically enter complex adaptive adversarial systems must be manned, trained, and resourced to leverage these new cyberspace opportunities. Those forces will change the preferences, sentiments, intentions, and interests of populations for decades to come.

15. SUBJECT TERMS

Data analytics, social media, systems theory, sociology, and contemporary U.S. Army and Joint Doctrine.

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
UNCLASSIFIED					
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	49	

MONOGRAPH APPROVAL PAGE

Name of Candidate: Major Sean P. Lyons

Monograph Title: Social Media Analytics: A New Approach for Cyberspace Enabled Understanding of Operational Environments

Approved by:

_____, Monograph Director
G. Stephen Lauer, Ph.D.

_____, Seminar Leader
Juan K. Ulloa, COL

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL

Accepted this 10th day of December 2013 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

SOCIAL MEDIA ANALYTICS: A NEW APPROACH FOR CYBERSPACE ENBALED UNDERSTANDING OF OPERATIONAL ENVIRONMENTS by MAJ Sean P. Lyons, 50 pages.

The purpose of this paper is to highlight the need to increase discourse within the Army on the impacts of cyberspace on operational environments. Current Army doctrine emphasizes network defense and offensive strike capabilities for cyberspace activities, but does not expound on focusing advanced analytical tools for increasing shared understanding of the cyberspace information environment; then using that understanding to solve problems existing in a dual cyberspace-land domain. Global interconnectedness and the speed of change demand a new approach. This research borrows from data analytics, social media, systems theory, sociology, and contemporary U.S. Army and Joint Doctrine. The paper uses the Army Design Methodology (ADM) to provide a common lexicon and model.

The question for operational artists given the explosion of information technology over the last ten years is, “How does the Army at corps level Joint Task Forces and below leverage cognitive information from cyberspace to create a more complete understanding of operational environments?” This monograph explores Social Media Analytics (SMA) as a capability for providing Army commanders and staffs with cyberspace tools for generating human centric understanding. The research addresses SMA applied to a gap in contemporary Joint and Army doctrine, and evaluates SMA as an approach to bridging that gap.

The gap analysis and approach provide evidence to the viability of SMA as a tool for increasing shared understanding within operational echelons for dual domain environmental framing. The capability fulfills a requirement using open sources of data enabling a high degree of distribution. The topic is pertinent for military practitioners because SMA, and user generated content in cyberspace, present opportunities to increase operational tempo and the adaptability of Army operational and tactical level echelons by providing near-real time understanding through trending. The Army echelons directed to physically enter complex adaptive adversarial systems must be manned, trained, and resourced to leverage these new cyberspace opportunities. Those forces will change the preferences, sentiments, intentions, and interests of populations for decades to come.

ACKNOWLEDGEMENTS

To my wife, thank you for all the sacrifices you have made to provide the six of us opportunities.

TABLE OF CONTENTS

ACRONYMS

ADM	Army Design Methodology
ADRP	Army Doctrine Reference Publication
CEMA	Cyber Electromagnetic Activities
CIA	Central Intelligence Agency
CJTF	Combined Joint Task Force
COP	Common Operational Picture
DARPA	Defense Advance Research Projects Agency
DOD	Department of Defense
FM	Field Manual
IC	Intelligence Community
IO	Information Operations
IP	Internet Protocol
IPB	Information Preparation of the Battlefield
ISI	Intelligence and Security Informatics
IT	Information Technology
JP	Joint Publication
JTF	Joint Task Force
MC	Mission Command
NSA	National Security Agency
OSINT	Open Source Intelligence
SMA	Social Media Analytics
SMS	Short Message Service

ILLUSTRATIONS

Page

TABLES

Page

INTRODUCTION

> Conflict by its very nature involves people, whether over resources, territory, or ideology. Technological advances may increase our reach, but the last 12 years of war have reinforced that lasting results hinge on understanding and effectively influencing populations.[1]
>
> — General Raymond T. Odierno

The question for operational artists given the explosion of information technology over the last ten years is, "How does the Army at corps level Joint Task Forces and below leverage cognitive information from cyberspace to create a more complete understanding of operational environments?" This monograph explores Social Media Analytics (SMA) as a capability for providing Army commanders and staffs with cyberspace tools for generating human centric understanding of operational environments. The research addresses SMA applied to a gap in contemporary Joint and Army doctrine, and evaluates the viability of SMA as an approach to bridging that gap. The topic is pertinent for military practitioners because SMA, and user generated content in cyberspace present opportunities; opportunities that must be leveraged by the forces directed to physically enter complex adaptive adversarial systems. As the Chief of Staff of the Army stated "…understanding social and cultural networks becomes just as important as the weapons we employ. Only then can we isolate enemies, identify centers of gravity, and achieve lasting results."[2]

---

[1]GEN. Ray Odierno, "The Force of Tomorrow," *Foreign Policy* (4 February 2013): 3, http://www.foreignpolicy.com/articles/2013/02/04/the_force_of_tomorrow (accessed 2 October 2013).

[2]Ibid., 6.

On 17 December 2010 Mohammed Bouazizi a vegetable vendor in Tunisia set himself on fire outside of a provisional headquarters building.[3] The actions of this individual ignited a tinderbox of socio-political frustration across North Africa and into the Middle East. The resultant regional instability and intensity of change caught the world by surprise and the Arab Spring was born. Western intelligence communities did not anticipate the speed of change brought on by the protests and activism of the many disenfranchised populations. New political dynamics in Libya, Egypt, and Syria presented fleeting opportunities that were missed because of a lack of strategic situational understanding. From 2010 to the present the United States defense enterprise worked hard to ensure population centric surprises of this magnitude will not occur in the future.[4]

From a geostrategic perspective the United State now maximizes technological advantages in cyberspace. The national level Intelligence Community (IC) understands the importance of the human dynamic in strategic, operational, and tactical environments. This requires the United States Army to remain adaptive and stay abreast with rates of global change. Current Army doctrine emphasizes network defense and offensive strike capabilities for cyberspace activities, but does not expound on focusing advanced analytical tools for increasing

---

[3]Rania Abouzeid, "Bouazizi: The man who set himself and Tunisia on fire," *Time* (21 January 2011): 1, http://content.time.com/time/magazine/article/0,9171,2044723,00.html (accessed 23 September 2013).

[4]From 2010 to the present, the U.S. Intelligence Community and Department of Defense (DOD) worked to increase national level capabilities to analyze user-generated content from social media. Examples include the National Security Agency new data center expansion in Utah, Central Intelligence Agency funding of the Recorded Future Company, and Defense Advanced Research Projects Agency, XDATA project.

shared understanding of the cyberspace information environment; then using that understanding to solve problems existing in a dual cyberspace-land domain.[5]

The kinetic reduction of conventional military systems or regimes no longer defines victory. Global interconnectedness and the speed of change demand a new approach for decreasing the number of unknowns and limiting ambiguity within operational environments. Success hinges on understanding relationships between regional and local actors, populations at multiple scales, and influences in order to answer questions like: What is the meaning of what we see? Where does the story begin and end? What happened, is happening and why?[6] Army doctrine provides models such as DIME, PMESII-PT, and ASCOPE to aid in generating holistic understanding.[7] Cyberspace provides opportunities to further decrease the number of unknowns and ambiguity within these models. If exploited, the same cyberspace capabilities used by the IC increases the adaptability of Army operational and tactical level echelons by providing a near-real time understanding through trending and forecasting of user generated content.

---

[5]In 2010 the DOD established United States Cyber Command and Army Cyber Command to face the emergence of cyberspace threats. As of March 2013 no unifying body of doctrine addresses the use of SMA within operational and tactical echelons. Presently cyber doctrine focuses on network defense and offensive strike capabilities. There is a void in resource application and doctrine for understanding the cyberspace-operating environment.

[6]Department of the Army, Army Doctrinal Reference Publication (ADRP) 5-0, *The Operations Process* (Washington, DC: Government Printing Office, 2012), 2-5. The three questions of ADM are an essential component of the iterative process of understanding. Although the three questions of the ADM are used throughout this work, this is the only citation.

[7]These acronyms represent components to Army planning models; elements of national power (Diplomatic, Informational, Military, Economic—Known as DIME), operational variables (Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time—known as PMESII-PT), civil considerations (Areas, Structures, Capabilities, Organizations, People, and Events—known as ASCOPE)

Social Media Analytics are a viable option as a tool for increasing shared understanding within operational echelons of dual cyberspace/land domain environmental frames. They offer as a capability, an open source intelligence methodology and cross-functional utility as a tool.

The purpose of this paper is to highlight the need to increase discourse within the Army on the impacts of cyberspace on operational environments at corps-level Joint Task Force (JTF) echelons and below. The focus is relational systems in cyberspace blended with the physical military land domain. This monograph illuminates a perceived gap in Army doctrine pertaining to the development of a dual cyberspace and land domain common operational picture. Social media analytics offer a research vehicle for reinforcing the capability requirement illustrative of the gap.

The scope of the monograph reinforces existing concepts, and provides new insights through a novel application of capabilities. The research borrows from data analytics, social media, systems theory, sociology, and contemporary U.S. Army and Joint Doctrine. The paper uses the Army Design Methodology (ADM) to provide a doctrinal lexicon and model. The research follows a highly technical and emergent field of study and focuses on a singular application, increasing accurate shared understanding of what ADM calls the environmental frame.[8] While analysis throughout this monograph centers on the United States Army, it is

[8]Department of the Army, ADRP 5-0, *The Operations Process*, 2-7. Chapter two provides detail on the entire ADM process building a common lexicon. Discussion of the environmental frame for context. "…operational environmental frames (using narrative and visual models) describe and depicts the history, culture, current state, relationships, and future goals of relevant actors in an operational environment. An operational environmental frame consists of two parts— the current state of the operational environment and the desired end state of the operational environment."

equally applicable to Joint organizations and sister services within the Department of Defense (DOD) as well.

There are governmental policy, public perception, and secrecy problem-sets that are beyond the scope of this research. These limitations are acknowledged and viewed as temporary hurdles in the adaptation of DOD cyberspace efforts. The intent here is to highlight an opportunity. Social Media Analytics, as a capability, is already proliferated, yet probably not to the point of saturation. Private industry is using SMA to increase understanding of environments and individuals can purchase the tools for private use.[9] Enemies of the United States have or will leverage these capabilities in the struggle to achieve an advantage in the information environment.[10]

Limitations to operational exploitation of this opportunity lie in doctrine. Doctrine is "what we do." Army-wide adaptation and funding of a concept will not occur unless captured by

---

[9]In concert with defense enterprise advancements private industry also applied information technology for greater understanding. Corporations are marketing SMA to other businesses and private entrepreneurs. The focus for major corporations are market shares and supply chain awareness. Companies like Google, IBM, Raytheon, Recorded Future, and others are invested in these capabilities. Their goal is to understand environments for increased profit margins and Return On Investment (ROI). For example methods of purchasing SMA for individual or business use visit the following websites; (Google) http://www.google.com/ analytics/apps/ results?category=Social%20Media%20Analytics (accessed 11 March 2013); (IBM) http://www-01.ibm.com/software/ analytics/solutions/customer-analytics/social-media-analytics/(accessed 8 March 2013); (Recorded Future) https://www.recordedfuture.com (accessed 20 March 2013).

[10]GEN. Ray Odierno, "The Force of Tomorrow", 6. "We must take full advantage of these technologies, building our own capabilities to operate in cyberspace with the same level of skill and confidence we enjoy on the land. We will either adapt to this reality or risk ceding the advantage to future enemies." This statement provided by the Chief of Staff of the Army reinforces the temporal component of cyberspace technological advantages.

the discourse of doctrine. Service doctrine feeds joint doctrine. Joint doctrine is a reflection of what each service brings to the fight and a compromise when roles overlap. This is why Joint and Army doctrine comprise a large portion of this monograph.

The research methodology highlights the history and utility of SMA as a capability. Then frames the problem (a capability gap) in the context of complex and adaptive operational environments using doctrine. An evaluation of SMA as a capability applied to the gap in doctrine is designed to address four different contexts; using the Haitian humanitarian relief effort of 2010, and the 2009 Iranian elections. Haiti represents the *active application* of the capability into an *open system*. Iran represents a *passive application* of the capability by observing a *closed system*. The selection of these two cases demonstrates how SMA use open sources of information in multiple environmental contexts.

Two baseline questions used during this evaluation determine the viability of SMA as a tool for generating greater understanding of dual cyberspace and land operational environments. First, can the capability provide the information required? Generally, this equates to answering the "three questions" of ADM, (What is the meaning of what we see? Where does the story begin and end? What happened, is happening, and why?). Specifically, this means the opportunity to understand systems in the cognitive dimension of cyberspace to anticipate change while recognizing and managing transitions.[11] Second, could the use of the tool help transcend organizational frictions identified in the gap analysis?

---

[11]Department of the Army, Field Manual (FM) 5-0, *The Operations Process* (Washington, DC: Government Printing Office, 2010), 3-2. These concepts are selected goals of the ADM.

Following the evaluation is a hypothetical scenario to illustrate recommendations for further research. The paper is structured in five parts following the introduction; SMA background, SMA capability, the problem in doctrine, analysis of an approach, and conclusion.

BACKGROUND TO SOCIAL MEDIA ANALYTICS

The story of SMA provides context and begins with the terrorist attacks against the United States on 11 September 2001. From this attack came a focused effort to leverage all available assets to prevent future attacks. One area of advancement was IT and the cyberspace domain. During the first decade of the 21st century data within the cyberspace information environment expanded at an alarming rate. To convert the available data into actionable information a new cross-disciplinary approach was taken. Information technology experts worked with academics in the fields of natural sciences, computational science, information science, social sciences, engineering, medicine, and the DOD.[12] The goal was to design methods and information requirements that could provide a framework for focusing analysis of massive amounts of structured and unstructured information.

Dr. Hsinchun Chen, from the University of Arizona's Artificial intelligence laboratory, is a leader in the cross disciplinary pursuit of data analysis from the cyberspace domain. In his 2006 book *Intelligence and Security Informatics for International Security*, Dr. Chen proposed the development of a formal cross disciplinary science of "Intelligence and Security Informatics"

---

[12]Dr. Hsinchun Chen, *Intelligence and Security Informatics for International Security: Information Sharing and Data Mining* (Integrated Series in Information Systems) (New York: Springer, 2009), 3.

(ISI).[13] The purpose was to further the "development of advanced information technologies, systems, algorithms, and databases for national security-related applications, through an integrated technological, organizational, and policy-based approach."[14] The concept of ISI did not develop in a vacuum, Dr. Chen and those like him helped to transition the process of analysis and synthesis of large volumes of data into an IT aided process using analytics.

Analytics in the simplest form are tools used to analyze otherwise unmanageable amounts of random data. They are software packages that use statistics based programs to structure, cluster, and visualize data.[15] Analytics not only make large volumes of unstructured data manageable they also provide the ability to increase predictive modeling. In parallel to the advancement of technologies for analytics came the theory of big-data, and the corresponding discipline of big-data analytics.

According to the National Science Foundation, big-data refers to very large diverse datasets drawn from any and all digital sources.[16] Big-data modeling uses extremely large sample

---

[13]Ibid., 2.

[14]Dr. Hsinchun Chen, "Artificial Intelligence Laboratory: Intelligence and Security Informatics," University of Arizona Eller College of Management, http://ai.arizona.edu/research/isi/ (accessed 4 June 2013). Information obtained from the research goals and mission listed on the ISI home page at Arizona University, 1.

[15]Most analytics programs are a blend of multiple tailored software tools. Each tool serves a purpose such as data extraction, linguistic analysis, data analysis, synthesis of information, and a method for visualization.

[16]NSF 12-499, Program Solicitation, "Core Techniques and Technologies for Advancing Big Data Science," *National Science Foundation* (1 October 2010): 3. "Big data" refers to large, diverse, complex, longitudinal, and or distributed data sets generated from instruments, sensors, internet transactions, email, video, click streams, and or all other digital sources available today and in the future.

sizes when testing statistical theories. The sample sizes of data used decrease the chance that outlying variables of a model will impact its validity. Thus, imperfect or partially understood data inputs (information) become feasible for use during modeling.[17] The most important change big-data theory brings is the idea that causation is secondary to correlation when analyzing relationships among variables (actors) within a system.[18] The micro trends and correlations obtained when analyzing greater volumes of information enable increased accuracy of predictive analysis through trending. The requirement to deconstruct a system for causation and then reconstruct for future probabilities decreases. This enables an increased speed of understanding cyberspace environments.[19]

During the early 2000s, the use of analytics for big-data analysis and understanding of cyberspace was devoted to information and network security concerns resident within the cyber domain itself. This focus remains today as evidenced by the March 2012 *Worldwide Threat Assessment of the US Intelligence Community*. In this document, produced by the Director of

---

[17]Kenneth Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think About the World," *Foreign Affairs* (May/June 2013): 30.

[18]Ibid., 32. Mayer-Schoenberger discusses, " From causation to correlation. This represents a move away from always trying to understand the deeper reasons behind how the world works to simply learning about an association among phenomena and using that to get things done."

[19]Office of Science and Technology Policy Executive Office of the President, *Obama Administration Unveils "big Data" Initiative* (Washington, DC: Office of Science and Technology Policy Executive Office of the President, 2012), 1**.** In March of 2012 the U.S. Government made big-data theory a priority releasing the "Big Data Research and Development Initiative." The purpose of the initiative was to: "advance state-of-the-art core technologies needed to collect, store, preserve, manage, analyze, and share huge quantities of data; harness these technologies to accelerate the pace of discovery in science and engineering, strengthen our national security, and transform teaching and learning; expand the workforce needed to develop and use Big Data technologies."

National Intelligence, the first listed threat to national security is cyber.[20] This is important because the argument could be made that the criticality of network defense maximizes cyber-based capabilities and constrains operational use of resources for other purposes.

During the end of the 2000s the use of analytics and large open source datasets in cyberspace switched from a network defense focus to a more broad based approach, emphasizing understanding human interactions and social networks. This occurred due to the development of Social media platforms that enable cyber social networking.[21] What has happened over the past four years and began with the Arab Spring demonstrated a need to understand what happened, what is happening and why. Analysis of indicators in cyberspace provides new opportunities for identifying these global trends as they emerge. Those opportunities produced a reaction within the U.S. National intelligence community that spurred further innovation of social media oriented big-data analytics programs.[22]

---

[20]James R. Clapper, "Worldwide Threat Assessment of the US Intelligence Community," Statement for the Record for Senate Select Committee on Intelligence (Washington, DC: Office of the Director of National Intelligence, 12 March 2013), 1.

[21]Common examples of platforms include Twitter, MySpace, Facebook and U-Tube. Additionally most departments and agencies of the United States government operate web pages that generate conversations and connections with the cyber world. This is also true for businesses, countries, inter-governmental organizations, and non-governmental organizations.

[22]Beginning around 2010 the department of defense and various intelligence agencies began partnering with small businesses and large corporations to create data analytic tools and databases that could make sense of all the information available using social media platforms. In 2011 the CIA private non-profit company, In-Q-Tel, helped start the analytics company Recorded Future. In 2012 as part of the White House big data initiative DARPA initiated the XDATA project. XDATA is a project that seeks to develop tools for managing increasingly large volumes of data gained from all types cyber based technologies.

In August of 2010 the Office of Naval Research conducted a socio-cultural based study on understanding networks and social interactions at the local level in Afghanistan. The study, *Sociocultural Data to Accomplish Department of Defense Missions,* represents a conceptual linkage between social networks in the cyberspace domain and population dynamics in the land domain. The research focused on human systems integration, unifying social frameworks, and cultural modeling. Cultural models viewed in terms of connections between language, symbols, rituals, and behavioral models.[23] A common theme in the study was the capture of the current socio-cultural environmental frame.[24] Networks and population linkages collapse over time rendering standard anthropological insight unhelpful.[25] Social media-based data could provide better understanding of current and future conditions because of the real-time nature of the information.

From 11 September 2001 through 2013 simultaneous innovation in the defense and business sectors increased cyber based analytical technologies. Big-data theory and analytics entered the common lexicon for business intelligence and national security. With the development of social media platforms and popularity of social networking the IT community gained a dual analytics focus.

---

[23]Department of the Army, ADRP 5-0, *The Operations Process,* 2-5.

[24]Ibid., 2-7.

[25]Robert Pool, Rapporteur, Planning Committee on Unifying Social Frameworks; National Research Council, *Sociocultural Data to Accomplish Department of Defense Missions: Toward a Unified Social Framework: Workshop Summary* (Washington, DC: The National Academies Press, 2011), 85.

SOCIAL MEDIA ANALYTICS DEFINED

The concept of SMA is not clearly defined as a universally accepted term. The term is often confused with "social network analysis," "web analytics," "data mining," "text analytics," or other areas of emerging research.[26] Social media analytics use all the aforementioned techniques. The target areas are human relationships and the correlation of those relationships to other data such as artifacts or events. Social media analytics focus on the cognitive dimension of the information environment and the social layer of cyberspace. The lack of a commonly understood definition presents a problem for generating understanding of the capability for broad military use. This section provides a working definition at the conclusion to generate perspective during analysis of SMA as a capability.

The confusion surrounding SMA as a capability centers on how *social media* is defined. The term social media is synonymous with Twitter, Facebook, and other mainstream social networking platforms. This view limits the utility of the term, because there are many more categories of platforms to consider. Social media are software applications with operating concepts based on the collaborative exchange of user-generated content.[27] Emphasis is on the

---

[26]Social network analysis, Adam Cooper, "A Brief History of Analytics," *CETIS Analytics Series* 1, no. 9 (2012): 10; Web analytics**,** Cooper**,** 6; Data mining, Department of the Army, ADRP 2-0, *Intelligence* (Washington, DC: Government Printing Office, 2012), 3-6; Text analytics, Hsinchun Chen, Roger HL Chiang, and Veda C. Storey, "Business intelligence and analytics: from big data to big impact," *MIS Quarterly* 36, no. 4 (2012): 1165-1188, 3.

[27]Andreas M. Kaplan and Michael Haenlein, "Users of the world, unite! The Challenges and Opportunities of Social Media," *Business Horizon, Kelly School of Business Indiana University*, 53 (2010): 59-68, 61. "Social Media is a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user generated content." Web 2.0 is the Internet transition from a simple static display of information to a collaborative exchange.

individual over the organization, displaying discourse in a virtual world. The ability of application users to generate and alter content is the critical component. Examples of social media categories include: Blogs; collaborative projects (Wikipedia); Social networking sites (Facebook); Content communities (YouTube); virtual social worlds (Second Life); and virtual game worlds (World of Warcraft).[28] These platforms and hundreds of others, when aggregated, create a virtual world representation of the physical environment. Social media understood through this frame provides a very broad set of platforms for applying analytics to open sources of user-generated content.

Much of the lack of clarity surrounding SMA is also due to the specializations of the analytics community. There are specialized analytics disciplines for most professions that use cyberspace. These disciplines search for specific information requirements, on select IT platforms, using highly refined tools. Each new toolset creates a catchy new name. If you query "analytics" using Google you will drown in niche academic and marketing terms. Yet, there is a common trend among them. If the desire is for greater understanding of cognitive information in cyberspace (social layer), they all use social media platforms to harvest data.

The analytics community consists of multiple fields such as: business intelligence, Web analytics, operational research, artificial intelligence and data mining, social network analysis, information visualization, and learning analytics.[29] Each discipline has a focus that overlaps with others in the pursuit of greater understanding of cyberspace data. Business intelligence is a good

---

[28]Ibid., 62.

[29]Cooper, "A Brief History of Analytics", 3.

example. Within the business community the goal is to increase profit margins and Return On Investment (ROI). This entails listening to data present in cyberspace to find, exploit, and analyze markets and supply chains. Business intelligence applications for analytic processes include: commerce and market intelligence, government and politics, science and technology, health and wellbeing, security and public safety.[30] Each application uses analytics from multiple technical areas or sub-disciplines to help businesses increase their ROI. These include but are not limited to: big data analytics, text analytics, web analytics, network analytics, and mobile analytics.[31] These processes all leverage specific IT for specific information requirements.[32] This level of specialization stovepipes data and decreases shared understanding of underlying trends. The field of social network analysis is an exception.

Social network analysis is a critical field to address when defining SMA. The key components in social network analysis are relationships among people. Common goals of social network analysis are answering questions such as: Who is influential? Who is powerful? What sub-groups exist? Who is engaged or disengaged?[33] Social network analysis carries the connotation of human relational link diagrams. The clearest example is an analysis of social

---

[30]Chen, Chiang, and Storey, "Business intelligence and analytics: from big data to big impact", 3.

[31]Ibid.

[32]Examples include: Using web analytics, how many people view an advertisement through click streams? Using network analytics, what product news is gaining attention? Using text analytics, what products are people talking about? The goals are increased marketing effectiveness and profit margins. These techniques tailor advertising and change consumer behavior.

[33]Cooper, "A Brief History of Analytics", 10.

networks on Facebook. Facebook platform-applications such as “friends” and “likes” grant access to view other people’s accounts and rapidly disseminate information to all contacts. From an analysis of these relationships networks and levels of interconnectedness appear. Yet, a fixation on one type of platform (social networking sites) is not optimal for developing a larger understanding of the cyberspace domain. Social media analytics include much more than the obvious social networking platforms and provide a greater ability to corroborate information.

A narrow interpretation of what social media platforms are causes confusion with defining SMA as a tool. Specialization of the analytics community also complicates the idea. The ability of social media based analytics to provide a more diverse group of datasets and to identify underlying trends or correlations are why companies like Google and IBM have transitioned to focusing on social media.

The utility of SMA is more than network analysis. Companies are combining virtually all of the sub-disciplines of the analytics community and focusing on the entire cyberspace social media architecture. In 2013 IBM developed their SMA package for business. Their framework is specially designed to leverage the social layer of cyberspace to increase ROI.[34] It provides what JP 3-13-1, *Information Operations* describes as a linkage between informational and cognitive

[34]IBM, *Social Media Analytics: Making Customer Insights Actionable* (Somers, NY: IBM Corporation, 2013), 7. The framework is a four-part model of Discovery, Assessment, Segmentation, and Relation. This enables users to visualize what groups and actors are talking about in cyberspace and their sentiments. Sentiments generated determine reach and proliferation of ideas. The data is segmented into geographic, demographics, influencers, recommenders, and detractors. The information is synthesized to produce individual or group affinities associations and correlations.

elements of the information environment. The IBM model goes beyond explicit network linkages to identify hidden trends.

Other companies such as Google, and Recorded Future take SMA a step further. These companies use their programs to focus on specific concepts. Google has over fourteen SMA programs that focus on ROI and managing a company's social media footprint.[35] Google platforms provide companies the ability to interact with actors in cyberspace to change consumer perception, behavior, and provide forecasting for decision-making. The company Recorded Future developed programs that use social media to generate a spatial and temporal element for population based forecasting.[36]

The utility of SMA is the human centric linkage of informational and cognitive elements of structured and unstructured data in cyberspace. The business industry demonstrated that open source applications of SMA achieve strategic market advantage using tactical methodologies. Given the friction in defining SMA and the clouded utility offered by the analytics and business intelligence community, it is necessary to propose a working definition. This definition incorporates the baseline analytics processes identified by IBM, Google, and Recorded Future.

---

[35]To access the Google homepage and view all of the available SMA consumer products go to the following URL http://www.google.com/analytics/apps/results?category= Social%20Media%20Analytics (accessed 11 March 2013).

[36]Staffan Truvé, "Big Data for the Future: Unlocking the Predictive Power of the Web," *Recorded Future* (2011): 11. Recorded Future's temporal analytics applications can detect emergent conflicts. It uses a five-part framework of harvesting, linguistics analysis, refinement, data analysis, and user experience (visualization). This collection of analytic tools enables users to monitor worldwide protests. This capability has become critical for multinational corporation supply chain management and asset security. The key elements are time and location based forecasting of probable disruptive population behavior.

Working Definition

Social media analytics are a collection of software applications used in combination to extract, analyze, and synthesize both structured and unstructured data resident on social media platforms within cyberspace. The groups of applications include but are not limited to social network analytics, machine learning programs, data mining tools, and natural language processing. Targeted datasets include text, video, photo, and audio. The scale of datasets analyzed range from individual IT devices or IP addresses to big-data clusters. Social media analytics focus on human interactions to understand discourse and correlation over causation. The purpose is to increase understanding of the information environment for forecasting and decision-making.

THE PROBLEM (GAP IN DOCTRINE)

United States Joint and Army doctrine provide a common lexicon and engine for professional discourse. This discourse enables leaders at all levels to decrease organizational frictions and maximize opportunities by making clear, concepts that are unfamiliar. Cyberspace as a global domain has entered the military lexicon, yet doctrine does not guide military practitioners towards maximizing the new associated opportunities. Current Army doctrine emphasizes network defense and offensive strike capabilities for cyberspace activities, but does not expound on focusing advanced analytical tools for increasing *shared understanding* of the cyberspace information environment; then using that understanding to solve problems existing in a dual cyberspace land domain. Brief passages in select Army Field Manuals address the

necessity to develop cyberspace Situational Awareness (SA).[37] Yet, contemporary doctrine lacks a discussion of social media and the idea of user-generated content. The literature that addresses tools and techniques similar to SMA are JP 2-01, *Joint and National Intelligence Support to Military Operations*, and ADRP 2-0, *Intelligence*. Army Doctrine Reference Publication 2-0 references data mining as a "planning consideration" for the intelligence War Fighting Function (WFF).[38] Additionally the document addresses cyber-enabled intelligence as a complementary intelligence capability. "The use of cyber-enabled intelligence facilitates an understanding of the threat's capabilities, intensions, potential actions, vulnerabilities, and impact on the environment."[39] Joint Publication 2-01 introduces the concept of cyber social networking along with Open Source Intelligence (OSINT). Unfortunately these concepts are encapsulated in one paragraph, at the end of the document, referencing link diagrams.[40] This level of discussion will not produce a discourse on using SMA or social networks for other than targeting. Broad understanding of the utility of a tool requires focused discussion of how the capability, applied at

[37]Department of the Army, TRADOC PAM 525-7-8, *The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028* (Washington, DC: Government Printing Office, 2010), 67. Definition of Cyber Situational Awareness: "The immediate knowledge of friendly, adversary and other relevant information regarding activities in and through cyberspace and the EMS. It is gained from a combination of intelligence and operational activity in cyberspace, the EMS, and in the other domains, both unilaterally and through collaboration with our unified action and public-private partners."

[38]Department of the Army, ADRP 2-0, *Intelligence*, 3-6.

[39]Ibid., 4-11.

[40]U.S. Joint Chiefs of Staff, Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: Government Printing Office, 2012), D-18.

critical points during the operations process can provide the greatest advantages and increase adaptability.[41]

In 2010 the deputy chief of staff, intelligence (CJ2) for the International Security Assistance Force (ISAF), then-Major General Flynn, provided a recommendation for the intelligence branch. Interpreted here as a move away from the organizational path dependency of effects based logic. He posited a conceptual shift, a new perspective for the intelligence targeting process, from *Find, Fix, Finish, Exploit, and Analyze* to *Find, Feel, Understand, Exploit, and Analyze*.[42] This shift provides a future approach to *understanding* the human element of environments, if broad operational force understanding of cyberspace analytics and social engineering methodologies occur. Currently doctrine does not emphasize this perspective pertaining to analytics, social media, and understanding of environments, a gap exists.

The gap is the unfamiliar application of a tool for building as opposed to supporting an operational approach or detailed plan. This gap prevents the synchronization of capabilities, organizations, and personnel during the operations process. The complexity of the military cyberspace domain, and organizational frictions are key contributors. This section analyses the complexity of the cyberspace domain, capability requirements resident in doctrine, and organizational frictions that create the perceived capability gap.

---

[41]Department of the Army, Army Doctrinal Reference Publication (ADRP) 3-0, *Unified Land Operations* (Washington, DC: Government Printing Office, 2012), 1-8. Discussion of the operations structure and operations process as the Army's common construct for operations.

[42]Robert Pool, Rapporteur, *Sociocultural Data to Accomplish Department of Defense Missions:,* 14.

The Cyberspace Domain

Friction exists at the intersection of military domains. Friction caused by constants such as DOD systems and personnel interoperability, but more importantly due to the rapid expansion of the information environment (cyberspace). The expansion of scope and composition of the information environment complicates models that create shared understanding. Concepts such as Joint Operations Areas (JOA) and Areas of Interest (AOI) double in complexity and cloud understanding of the operational environment because of the unbounded nature of the cyberspace domain.[43]

> The Joint Forces Commander's operational environment is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment (which includes cyberspace). Included within these are enemy, friendly, and neutral systems that are relevant to a specific joint operation.[44]

The definition provided by JP 3-0, *Joint Operations* takes the four service aligned traditional military environments of space, atmospheric, terrestrial, and maritime, and assigns them as areas of both operations and responsibility.[45] The transition from military environments

---

[43]U.S. Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, 2011), GL-5, GL-6. Area Of Interest—"That area of concern to the commander, including the area of influence, areas adjacent thereto and extending into enemy territory. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission." Joint Operations Area—"An area of land, sea, and airspace defined by a geographic combatant commander or subordinate unified commander, in which a joint force commander (normally a joint task force commander) conducts military operations to accomplish a specific mission."

[44]Ibid., xv.

[45]Isaac R. Porche, et al., eds, *Redefining Information Warfare Boundaries for an Army in a Wireless World* (Santa Monica, CA: RAND Corporation, 2013), 4.

dominated by service proponents to domains that cross component responsibility creates domain overlap. The overlap is where service culture and systems friction are highest. Domain overlap is more contested with the addition of the intangible geography of cyberspace.

> Cyberspace is a global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[46]

Cyberspace exists within all four traditional domains and retains the capacity as a component of the information environment to foster a virtual world. These unbounded virtual worlds double the requirement to understand any given bounded geography such as JOA, and AOI. The virtual worlds warrant discussion because they retain cognitive relationships that are often invisible in the physical environment. Within cyberspace individuals can possess multiple cyber personas and traditional sociocultural networks can be modified.[47] A closed antagonistic society in a physical area can present alternative sets of norms, values, and artifacts in a virtual world. Thus cyberspace can provide a version of an otherwise inaccessible physical environment. Often this version represents a more accurate representation of individuals and populations. A focus on the overlap of land and cyberspace domains is critical.

Using the ADM structure as context, the complexities of cyberspace and dual domain understanding are more apparent. The requirement for understanding increases, as do

---

[46]U.S. Joint Chiefs of Staff, JP 3-0, *Joint Operations*, iv-2.

[47]Department of the Army, Field Manual (FM) 3-38, *Cyber Electromagnetic Activities (CEMA)*, (DRAFT) (Washington, DC: Government Printing Office, 2013), 3-9. Cyber persona is a term used to illustrate the complexity of multiple identity and ownership of cognitively generated data in cyberspace.

opportunities. Army Design Methodology attempts to frame the operational environment by analyzing the current state in relation to a desired state. When incorporating the virtual world of cyberspace the number of environmental frames will double. The cyberspace environment adds another current-state (what things look like now) and a desired cyberspace-state (what we want to see and hear). The two separate environmental frames can then be blended or compared. Comparison akin to mirroring provides adaptability by identifying emergence or change when the environments are juxtaposed over each other. Additionally, when the cyberspace environmental frame develops in isolation, that separate perspective of the overall operational environment becomes a basis for gauging measures of performance and effectiveness of an implemented operational approach. Blending of the two domains increases accuracy when answering; "What is the meaning of what we see? Where does the story begin and end? What happened, is happening and why?"

The overlap of the military land domain and cyberspace adds a level of complexity to understanding the operational environment. An analogy of the complexity is to say that there are two operational environments one physical and one virtual. The symbols, historical events, and artifacts of both environments require understanding.[48] This discussion of domains is a key component to keep in mind when analyzing capability requirements and contemporary military doctrine.

---

[48]Department of the Army, ADRP 5-0, *The Operations Process*, 2-5. These terms are taken from the discussion of *narrative* construction.

Capability Requirements

Joint and Army *operations and planning* doctrine lack a discussion of specific methodologies to generate understanding of cyberspace, or cyber SA. Practitioners must analyze *functionally specific* doctrine for clarity of methods and tools. Numerous military disciplines play a part in generating understanding of environments during the operations process. Most are focused on providing a piece to the puzzle. These pieces are answers to specific questions in support of an approach or detailed plan. The doctrine of Mission Command (MC), Information Operations (IO), and Cyber Electromagnetic Activities (CEMA) represent cross discipline bridges for a discussion of cyberspace. An analysis of MC, IO, and CEMA speaks softly of a requirement to provide shared understanding of dual environmental frames in pursuit of a common operational picture. A gap in doctrine appears when tools are applied to build shared understanding for environmental framing, of the cognitive dimension of the information environment, within the social layer of cyberspace. This is because it is an unfamiliar application of a tool across two domains and multiple functional area disciplines.

Mission Command is the guiding philosophy within the US Army operating concept. The theory of MC is central to how the Army and by default Joint forces execute operations. This idea is important, because a lack of synchronization of capabilities, organizations, and personnel exists during the operations process pertaining to the cyberspace domain. An examination of ADRP 6-0, *Mission Command* highlights the critical capability requirement to create shared understanding

that spans the breadth and depth of the Army.[49] This entails socializing information vertically and horizontally, spanning multiple services and domains, while pulling from and pushing information to external organizations and commands.[50] The theory of MC represents an organizational forcing function for blending information; the mechanism used is the Common Operational Picture (COP).

Mission Command as a war fighting function uses the COP as a tool for blending and socializing operationally relevant information for the execution of staff tasks such as; conduct knowledge and information management, conduct inform and influence activities, and to conduct cyber electromagnetic activities.[51] "Through the mission command war fighting function commanders integrate the other war fighting functions into a coherent whole to mass the effects of combat power at the decisive place and time."[52] Mission Command as the nucleus of Intelligence, Protection, Movement and Maneuver, Fires, and Sustainment efforts illustrates a capability requirement to maintain situational awareness and understanding of the operational environments across the breadth and depth of all the military sub-disciplines. An issue becomes a

---

[49]Department of the Army, Army Doctrinal Reference Publication (ADRP) 6-0, *Mission Command* (Washington, DC: Government Printing Office, 2012), 2-13. To create shared understanding of the environment commanders and staffs use operational variables (political, military, economic, social, information, infrastructure, physical environment, and time—known as PMESII-PT) and the mission variables (mission, enemy, terrain and weather, troops, and support available, time available, and civil considerations—known as METT-TC) to aggregate relevant information.

[50]Ibid.

[51]Ibid., 3-2.

[52]Ibid., 3-1.

lack of discourse on what or how to generate that shared understanding of cognitive information from the cyberspace virtual environment using a COP.

In addition to the capability requirements within MC the doctrine of Information Operations (IO) provides a model for understanding the critical human-centric element of the information environment. The three dimensions to the information environment are the cognitive, informational, and physical.

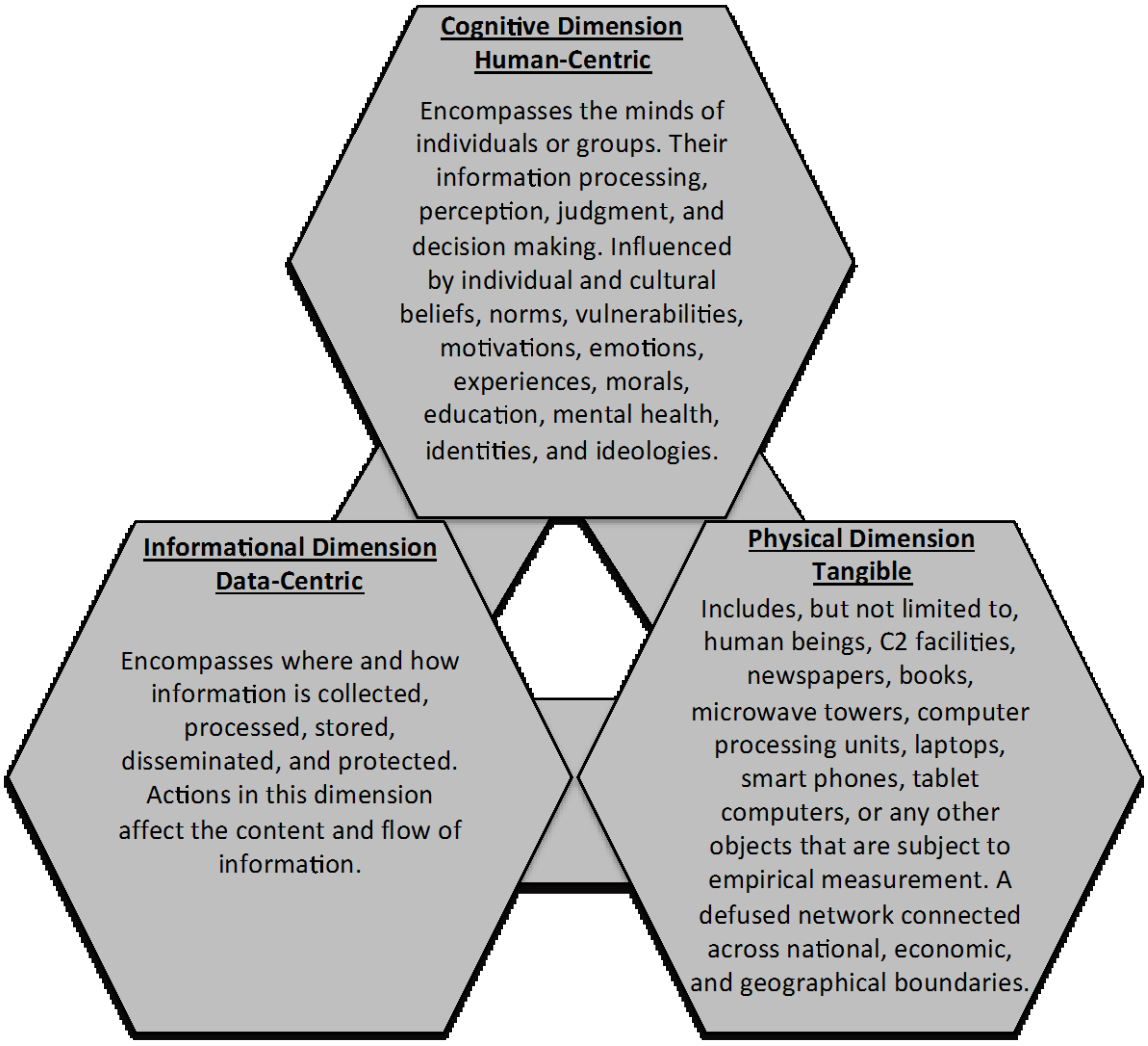

Figure 1. 3 Dimensions of the Information Environment
Source: U.S. Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: Government Printing Office, 2012), I-1, I-2, I-3.

The cognitive dimension is the decisive component for generating increased understanding of the human element. This provides the forum for understanding and means for application of effects to influence or modify human behavior. To accurately apply effects to this cognitive dimension requires holistic understanding of the data resident in the informational dimension of the environment. Currently, Army operational forces can only generate shared understanding of the physical dimension of the information environment using sensors and tools that operate within the physical domains (Air, Land, Sea, and Space). The intelligence driven IPB process and running staff estimates ensure socialization and incorporation of the physical aspects of the information environment within the COP. It is the understanding of the cognitive and informational dimensions together that present difficulties. While the information environment can exist in an analog world void of the Internet and modern IT, cyberspace is a manmade domain and requires greater focus.

US Army Cyber Electromagnetic Activity (CEMA) doctrine FM 3-38 provides a discourse on the physical and informational dimensions of the information environment within cyberspace. Currently FM 3-38 is the only socialized cyber specific piece of Army doctrine. It acknowledges an Army wide requirement to generate increased cyber based human-centric informational and cognitive understanding. Who has ownership of this task is not discussed.

> Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the

> electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system.[53]

Cyberspace Electromagnetic Activities consist of cyberspace operations, electronic warfare, and electromagnetic spectrum management operations. One of the critical tasks assigned to CEMA is the requirement to gain situational understanding.[54] The discussion of what CEMA provides to the COP pertaining to situational understanding is based heavily on friendly forces networks and platforms.[55] Paragraph 1-32 of FM 3-38 defines the CEMA methods for providing situational understanding. The focus is on capabilities that enable dissemination of the COP like Blue Force Tracker (BFT), Command Post of the Future (CPOF), and Force XXI Battle Command Brigade and Below (FBCB2).[56] These are all communications platforms that use the electromagnetic spectrum. Emphasis placed on generating increased cyber based human-centric informational and cognitive understanding is not present as a direct component of this task.

The discourse within FM 3-38 (CEMA) is a depiction of cyberspace as a layered domain to emphasize the need for an additional capability. The layers consist of the physical, logical, and social. This mirrors the three-dimensional model of the information environment with a focus on cyberspace. The figure below illustrates these layers.

---

[53]Department of the Army, Army Doctrinal Reference Publication (ADRP) 3-0, *Unified Land Operations*. Washington DC: Government Printing Office, 2012, 3-3.

[54]Department of the Army, FM 3-38, *CEMA* (DRAFT), 1-6.

[55]Ibid., 1-7.

[56]Ibid.

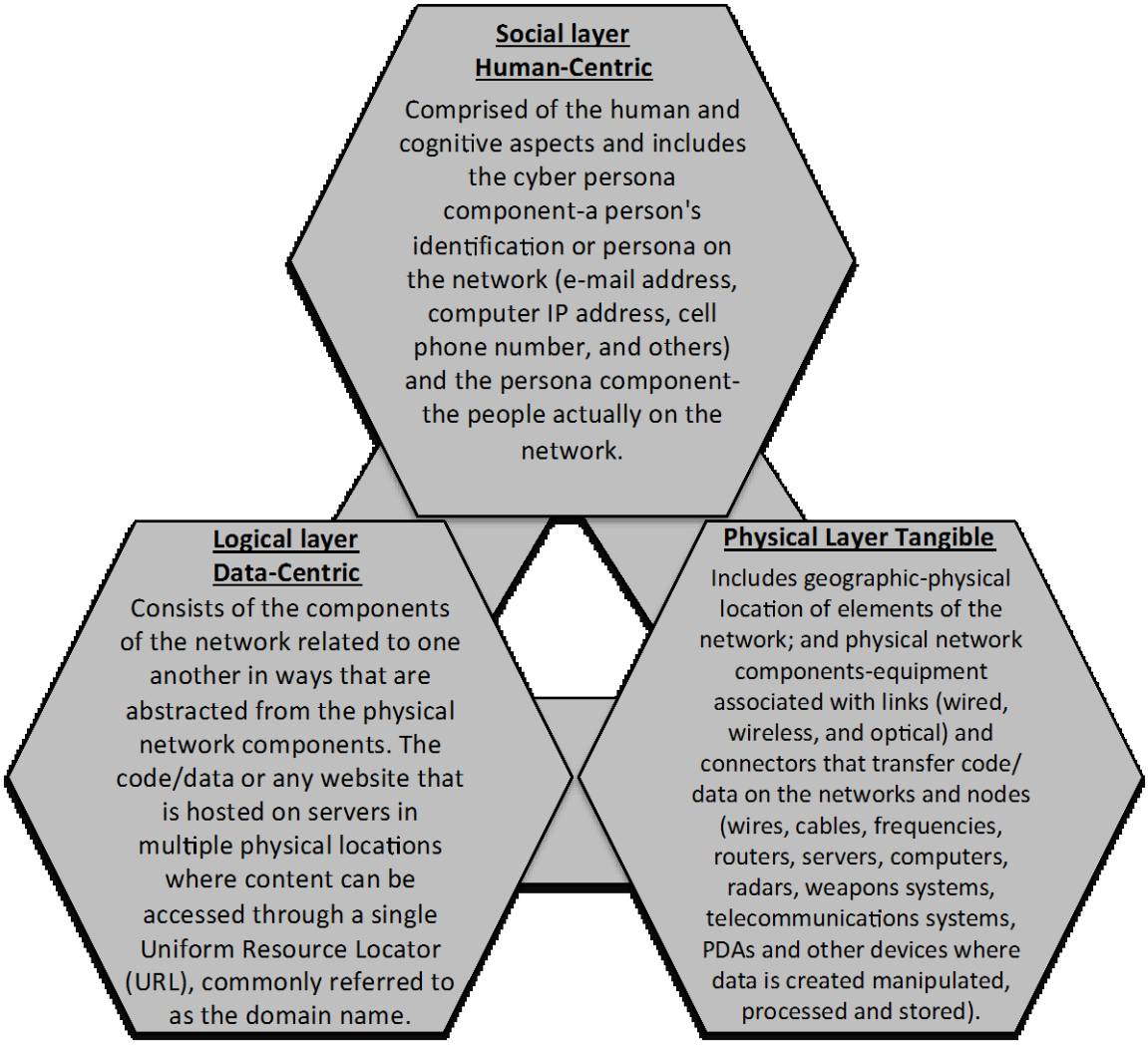

Figure 2. Layers of Cyberspace

Source: FM 3-38, 3-9. The illustration uses language presented and blends the definitions forming the CEMA layer trinity.

The layers of cyberspace highlight the requirement to holistically understand dimensions of information within the manmade cyberspace domain. The model used in CEMA is a method

for categorizing effects-based targeting. The five categories are physical, functional, cognitive, logical, and social characteristics.[57] The preponderance of CEMA focuses on targeting and the delivery of effects for offensive, defensive and information network operations.[58] The focus is further divided into external and internal friendly network targeting. Thus, the nature of CEMA operations creates a tendency to fixate on the physical and logical layers of cyber space. The social layer, just like the cognitive dimension of the information environment is sacrificed.

The requirement to understand the social layer still exists. Evidenced by standard intelligence driven planning processes. The IPB process relies heavily on developing shared sociocultural understanding of the operating environment. The Intelligence discipline uses a model called ASCOPE (areas, structures, capabilities, organizations, people, and events) to develop civil considerations and sociocultural understanding of physical domains.[59] During the recent wars in Afghanistan and Iraq requirements for sociocultural understanding far surpassed anthropological studies for making sense of the operational environment.[60] Current near-real time knowledge of the sociocultural environment was needed.[61] The information environment and CEMA indicate this requirement now transcends the physical domains into manmade cyberspace. With an exploration of the military cyberspace domain and critical capability requirements it is

---

[57]Ibid., 3-10.

[58]Ibid., 3-7.

[59]Department of the Army, ADRP 2-0, *Intelligence*, 2-5.

[60]Robert Pool, Rapporteur, *Sociocultural Data to Accomplish Department of Defense Missions:*, 85.

[61]Ibid., 31. This deduction is extracted from a discussion of the inability of socio-cultural understanding to arrive at the action level on the ground within the environment (Afghanistan).

necessary to address how the Army is organized to deal with the impact of cyberspace as an expanding environment.

Friction of Focus and Organization

There are two problems with the unfamiliar application of tools across two domains and multiple functional area disciplines, friction in operational area focus, and friction within Army functional area missions. Both of these conflicted organizational problems prevent the Army from adequately adapting to cyberspace expansion. Thus the capabilities required to frame dual domain environments and provide shared understanding (other than friendly forces) are missing.

Within the DOD and IC there are sub-communities with overlapping missions and areas of focus. Labeled here as communities of effort because they span multiple services, agencies, and departments yet retain the same professional focuses. Examples are cyberspace operations, intelligence operations, and information operations. Cyberspace operations are comprised of missions within Cyber Command, the service specific cyber commands and their forward support cells. Intelligence operations consists of activities conducted by national intelligence agencies, DOD level intelligence organizations, and service specific elements. Information operations play a role in the mission sets of both cyber and intelligence. The Army IO community referred to as a military functional area is comprised of six subordinate mission areas. Each of the three communities of effort (INTEL, CYBER, and IO) have requirements to leverage resources to accomplish specific missions within the cyberspace domain.

The cyber community creates network awareness, understanding of the physical layer of cyberspace, and maintains freedom of action while denying the same to adversaries.[62] The intelligence community focuses on the informational or logical layer gaining situational understanding of environments to provide decision makers relevant and quality information. The information operations community looks at all three with a doctrinal emphasis on the cognitive or social layer. These areas of focus overlap within a single domain and create friction caused by resource competition and mission primacy as influences range from governmental agencies, DOD commands, to functional areas.

The friction increases when applied to Army operational force functional areas and their corresponding mission focuses within the cyberspace domain. The table below depicts current doctrinal overlap of operational functions and focused technical functional areas.[63]

[62]U.S. Strategic Command, "U.S. Cyber Command Mission Statement," 23 June 2009, http://www.arcyber.army.mil/org-uscc.html (accessed 12 July 2013)**.**

[63]Isaac R. Porche, III, et al., eds, *Redefining Information Warfare Boundaries for an Army in a Wireless World* (Santa Monica, CA: RAND Corporation, 2013), 16. Table 1 of this monograph is constructed using the data of table 2-1 from the RAND document (Doctrinally Defined Functional Areas).

Table 1. Doctrinally Defined Functional Areas

Functional Area	**Selected Subareas, Divisions, and Activities**
Electronic Warfare (EW)	Electronic attack (EA), electronic protect (EP), electronic warfare support, spectrum management and control
Computer network Operations (CNO)	Computer network attack (CAN), computer network exploit (CNE), computer network defense (CND)
Network Operations	Information assurance (IA)
Electromagnetic Spectrum Operations (EMSO)	Spectrum management, frequency assignment
Information Operations (IO)	EW, CNO, PSYOP, MISO, OPSEC, MILDEC
Signals Intelligence (SIGINT)	Gathering intelligence by intercepting signals
Military Information Support Operations (MISO) formerly psychological operations	Influencing emotions, motives, objective reasoning, and behavior
Public Affairs	A focus on U.S. forces, populations, coordinating with MISO but remaining separate
Knowledge management	Creating, organizing, applying and transferring knowledge

Source: Created by author

All of the listed functional areas operate in the cyberspace domain. Using the three-dimensional model of the information environment it appears they all focus on the physical and informational dimensions. The exceptions are MISO, PA, PSYOPS, and MILDEC. With the addition of Cyber Electromagnetic Activities in 2013, there are five areas that possibly focus on the cognitive dimension. These niche focus areas do not carry the weight required to automatically gain access to the "team" when building an approach to solving unfamiliar

problems in unprecedented dual domain environments. It is logical to conclude that marginalization of the cognitive dimension will occur during environmental framing.

Friction within functional areas also exists in terms of modern relevancy, organizational structure and mission focus. A 2013 RAND Corporation study examined Army resources used within cyberspace and concluded that the greater information environment in which all of the aforementioned functional areas focus should be simplified into technical and psychological dimensions.[64] The study advocated the adaptation of Information Warfare as a doctrinal term to codify the effort to streamline the application of functional areas to the cyberspace domain. The study evidenced a lack of common vision for Army Information Operations.[65] A systemic problem is the tendency to view subordinate functional areas through separate lenses. The result is less attention devoted to the possibility of integrating supporting or related capabilities or to value that might be added by capabilities outside of the functional area.[66]

The frictions in operational area focus and functional area missions create an organizational problem. The problem is an inability to satisfy the capability requirement to apply niche discipline toolsets in an unfamiliar manner across two domains and multiple functional areas. Who is responsible for providing shared understanding of psychologically analyzed human behavior from the social layer of cyberspace when the information is extracted using signals intelligence within the electromagnetic spectrum? This question highlights the problem with applying current doctrine using existing organizational structures.

---

[64]Ibid., iii.

[65]Ibid., 25.

[66]Ibid., 23.

The Gap

Complexities of domain overlap and organizational frictions prevent the synchronization of capabilities, organizations, and personnel during the operations process. A gap appears when viewed in light of capability requirements highlighted in MC, IO, and CEMA doctrine. The gap is the unfamiliar application of a tool for building as opposed to supporting an operational approach. Current doctrine does not provide any practical answers. Who owns the human centric analysis of relationships in cyberspace? Where do commander and planners go to rapidly gain and maintain access to this dynamic information? How do they answer those three questions, for the cyberspace domain (What is the meaning of what we see? Where does the story begin and end? What happened, is happening, and why?)? There are tools to gain this understanding readily available for off the shelf procurement. It is possible that social media analytics are a viable option.

ANALYSIS OF AN APPROACH

How does the Army at corps level JTFs and below leverage information from cyberspace to create a more complete understanding of environmental frames? This question identified a perceived gap in contemporary Army doctrine. A lack of discourse exists on the utility and cross-functional applicability of cognitive information gained from cyberspace. Across the Army this creates an unfamiliar problem for planners and commanders.

The analysis of SMA as an approach uses two cases (Haitian earthquake of 2010 and Iranian elections of 2009). Haiti is an example of how available social media was not effectively used during a humanitarian crisis because analytic programs to effectively aggregate and make sense of the available information did not exist. Thus, given the gap in doctrine and what we do as an Army the Haitian case represents the current state of operational and tactical use of the platforms. The Iranian case is an example of the desired state or where the army needs to be with

regards to understanding cognitive information in the cyberspace domain. To determine the viability of SMA as a tool for generating greater understanding of dual cyberspace and land environmental frames the following questions are used: (1) Can the capability provide the information required? Generally, this means providing answers to the "three questions" (What is the meaning of what we see? Where does the story begin and end? What happened, is happening, and why?). Specifically, this means the opportunity to understand systems in the cognitive dimension of cyberspace to anticipate change while recognizing and managing transitions; (2) Could the use of the tool help transcend organizational frictions identified in the gap analysis?

Haitian earthquake of 2010 (Open System)

The Haitian earthquake of 2010 is an example of organizations both governmental and private using the platform of social media for communication purposes during crisis. This represents the utility of the platforms, as they are understood in doctrine today. On 12 January 2010 a 7.0 magnitude earthquake struck the country of Haiti. The capital of Port-au-Prince and other population centers were devastated with an estimated 230,000 killed, 300,000 injured and a million displaced.[67] The United States deployed a Joint Interagency Task Force, JTF Haiti to assist. JTF Haiti was one of the first operational units of the DOD to use social media to communicate both externally and internally leveraging the cyberspace information environment.[68] This developed in concert with civilian and international relief agencies doing the

[67]Dave Yates and Scott Paquette, "Emergency Knowledge Management and Social Media Technologies: A Case Study of the 2010 Haitian Earthquake," *International Journal of Information Management* 31, no. 1 (2011): 6-13, 4.

[68]Ibid., 7.

same. All agencies involved understood the communications capabilities offered by social media. As chaos and complexities of the disaster took hold, human adaptability pushed social media as an emergent disaster response tool for all involved actors.

JTF Haiti entered an open complex adaptive system as both a supporting and supported member of an international effort. An ad-hoc assemblage of relief organizations and preexisting United Nation forces were on site. Collaboration with and awareness of other actors was at a premium. The JTF became aware of the requirement to gain near real time understanding of the environment for crisis planning and to develop a common operational picture.

During Haiti the requirement for SMA existed, yet the capability in 2010 was not developed to the point of operationalization. Both disaster victims and relief workers used social media to communicate and better understand the environment. The preponderance of all information used from social media by JTF Haiti and other relief organizations was open source data. The most widely used platforms were the UN inter-agency OneResponse Website, the Sahana Free and Open Source Disaster Management System, and the crowd- sourcing platform Ushaidi.[69] Each of the platforms provided critical user generated information. Examples included locations of suspected trapped personnel, status of aid distribution sites, and sentiments of the population clusters.[70] Each piece of information provided an *opportunity* to aggregate and trend cognitive information to develop a near real time current state of the environment.

---

[69]Julie Dugdale, Bartel Van de Walle, and Corinna Koeppinghoff, "Social Media and SMS in the Haiti Earthquake," proceedings of the 21st international conference companion on World Wide Web, 713-714; ACM, 2012, 713.

[70]Ibid.

Major problems appeared with social media use during the disaster coordination efforts because of the unfamiliar nature of extracting actionable information from cyberspace. In a 2012 study titled "Social Media and SMS in the Haiti Earthquake" researchers examined the Short Message Service (texting/blogging) and other social media platforms used by organizations during the disaster. The research concluded:

> Information from citizens via social media and SMS proved useful in Haiti, particularly when it was aggregated at an area level. However there were problems: information overload; questionable speed of information delivery; difficulties of processing information in a non-standard format from different sources and in various languages; the complexity of managing volunteer communities; and the very limited value of using information at the street level.[71]

Of particular importance was the reliability of information at the street level. On average SMS and other reporting platforms retained a very low rate of accurate information. This was partially attributable to the emotional state of the individuals posting the information. Locations of trapped loved ones and even depleted aid stockpiles at distribution nodes were 80-90 percent inaccurate.[72] The information presented by the social media platforms from the populations to organizations providing disaster relief lost its meaning and importance due to inaccuracy. These problems stemmed from a lack of SMA to make sense of all the unstructured data sets and to establish trends.

An examination of a 2010 action research report *Emergency Knowledge Management and Social Media Technologies: A Case Study of the 2010 Haitian Earthquake* by Dave Yates and Scott Paquette points to the emergent power of social media during crisis. Their study

---

[71]Ibid., 714.

[72]Ibid.

concluded that the importance of social media as a platform for cognitive information is critical. Social media provided contextual information that responding organizations and the public used to make sense of the environment.[73] Although JTF Haiti realized the capability of social media they used it predominately as an internal communications conduit. The various subordinate organizations and functional areas communicated on wiki and SharePoint collaborative social media platforms.[74] This encouraged cross-boundary communication between groups with different tasks and roles.[75] Social media was used to support execution of operations through communication as opposed to understanding the environment. The JTF lacked an organizational structure that could focus on the cognitive dimension of information from cyberspace. A concerted effort to aggregate cognitive data from platforms to extract underlying trends was missing. The emergent importance of social media during the disaster was not anticipated.

The use of social media in Haiti was essentially a first for a JTF. The mission was population focused with a heavy reliance on new IT. Cyberspace emerged as a critical component to the larger environmental frame of the system. Information was available for answering the "three questions" yet the capability to translate that information was not present. The Haitian case allows for several deductions to be made. The first is that social media was an enabling knowledge management and communication capability for JTF Haiti and other organizations. There were frictions with managing/distilling large quantities of unstructured data then

---

[73]Dave Yates and Scott Paquette, "Emergency Knowledge Management and Social Media Technologies:", 3.

[74]Ibid.

[75]Ibid., 8.

aggregating and making sense of the information. This points to the viability of SMA as a tool for generating greater understanding of the cyberspace environment in Haiti. It is possible that contemporary SMA applied to the Haiti effort could have eliminated some organizational frictions. Collaborative planning by all stakeholders viewing the same cyberspace COP might have increased understanding of the dynamic physical domain of Haiti.

Iranian elections of 2009 (Closed System)

The country of Iran is a closed system. Western nation physical access to the country is highly restricted and indirect access to the population is difficult at best. To develop a holistic understanding of internal system dynamics alternative methods are required. In 2009 social media platforms emerged in Iran and provided an opportunity to frame the dynamic domestic system of Iran through the application and use of SMA tools and techniques.

During the summer of 2009 Iran held its tenth presidential election. The 2009 elections were significant because the internal dynamics of the country changed. A formal opposition group emerged within the system. This change presented an opportunity and a requirement to understand the nature of the new system as seen through cyberspace. "On June 12, 2009, Islamic Republic–controlled media announced a surprise landslide reelection victory for Ahmadinejad only hours after the polls closed."[76] A large portion of Iranian people viewed the voting process as fraudulent. Accusations were made against the victor, President Mahmoud Ahmadinejad and the government. Protests and civil unrest occurred for nine months post-election calling for the

[76]Douglas Yeung, et al., eds., *Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election* (Santa Monica, CA: RAND National Security Research Division, 2012), 14.

removal of the president.[77] As a result of the contested election the Green Movement emerged as a new internal actor in opposition to the Iranian government.

> The Green Movement relied heavily on Twitter, Facebook, text messaging, and the thousands of blogs created by ordinary Iranians to quickly organize and coordinate opposition efforts and public demonstrations, as well as to disseminate doctrine and political manifestos. These social media tools played a pivotal role in the drive to circumvent government censorship and secure broad support from different, often conflicting, strata within the Iranian populace.[78]

In 2012 the RAND Corporation created a technical report on the use of a social media analytic program call Linguistics Inquiry and Word Count (LIWC). Their study used this early form of SMA and applied it to the 2009 Iranian election. Analytics applied to twitter proved viable for understanding foreign public sentiment on political topics.[79] "The relative anonymity of the Internet and social networking sites has given people living in societies with restricted freedom of expression an outlet to express forbidden views."[80] The study identified that SMA as a capability provided the opportunity for greater forecasting of the Iranian population and political environment.

---

[77]Ibid., 14. The green movement was a broad based Iranian government opposition group: "The Green Movement (Jonbesh e Sabz) was born directly of this opposition to Ahmadinejad's reelection. The two reformist presidential candidates, former Prime Minister Mir Hussein Mousavi and former Parliament Speaker Mehdi Karroubi, emerged as its leaders."

[78]Ibid.

[79]Ibid., xii.

[80]Ibid., 2.

> Ultimately, we (RAND) view LIWC and other automated content analysis as an important part of research designs for studies of countries in conflict generally (such as Pakistan or Egypt, as well as Iran)—both to examine them on their own terms and to make comparisons between them.[81]

The RAND study found five viable areas that SMA generated greater understanding through harvesting cognitive dimensional information from cyberspace. These included: enable analysts to assess the impact of political events on public opinion; forecast important events in countries of interest; inform outreach efforts in foreign populations; help the U.S. military understand and engage people in its areas of operations; pin point intelligence gaps.[82] These findings translate into the capability to develop more complete environmental frames for planning. The RAND research team used analytics to reduce the manual analysis of unstructured open source text data. This relatively small niche research topic generated synthesized information with policy level implications. The study aggregated large volumes of text, processed the data, and delivered decision level information about the Iranian environment. The complexity of the environment was reduced by providing answers to what happened, is happening, and why? Without the use of cyberspace common understanding of the Iranian environment was marginal at best. This research represents the unfamiliar application of a tool to provide shared understanding of psychologically analyzed human behavior from the social layer of cyberspace.

The nature of the closed Iranian system, the 2009 elections, and the use of social media by the Green Movement demonstrated how cyberspace emerged as a critical component to a larger environmental frame. Social media platforms provided cognitive information for answering

---

[81]Ibid., xviii.

[82]Ibid., 4.

the three questions. The SMA tool of LIWC retrospectively provided answers otherwise unattainable. The Iran case and RAND Corporation study allow for the following deductions to be made. Social Media platforms are viable sources of cognitive information for generating greater understanding of closed systems. Social media analytics could identify emergence in a system if structure and organizations are in place to capitalize on the available information when created in cyberspace. Trending and forecasting offered by SMA as defined in this monograph could aid in anticipating change while recognizing and managing transitions. The RAND study is a representation of where the Army needs to be with regards to generating understanding of dual cyberspace land domain environmental frames.

Results and Issues

The Haiti case highlights the need for SMA as a capability at JTF levels within operational environments. The Iranian case validates rudimentary SMA as an option for creating greater understanding of dual cyberspace and land domain environmental fames. Answers to the three questions of the Army Design Methodology are aided by the application of SMA. It appears that SMA as a capability can address some of the specific requirements to understand systems in the cognitive dimension of cyberspace to anticipate change while recognizing and managing transitions.

Social media analytics are designed to operate using open sources of information freely available in cyberspace. This is similar to Open Source Intelligence (OSINT) methodologies. A reliance on open source cognitive dimensional cyber data is more readily shared than stove-piped classified intelligence products from national level intelligence organizations. Given the limited security caveats required using open sources of information collaboration could be increased using SMA as a capability. Multinational partners, nongovernmental organization, even multinational corporations are better integrated when information flows freely.

Social media analytics as a capability create the opportunity to address the frictions of focus and mission identified in the gap analysis of this monograph. The nature of the tool as a software application is a promising aspect in terms of distributive capacity. The similarity to OSINT methodologies plays a large part in this. Social Media Analytics can help synthesize information for rapid vertical and horizontal socialization within an organization. Simultaneous collaboration by multiple headquarters in a JTF, supporting organizations, and diverse functional areas is a possibility. Frictions of focus and mission could be reduced through increased collaboration using a common picture of the cyberspace environment. As JTF Haiti showed, social media itself is a platform for distributing the shared understanding of a COP.

Analysis of SMA as an approach identified a significant issue. Both the Haiti and Iran cases dealt with very large and diverse unstructured datasets in cyberspace. To archive and maintain a pulse of this cognitive dimensional information on a global scale is resource intensive and complex. More than likely it is beyond the scope of what a JTF can do. It appears that Army echelons below corps size will have difficulty rapidly building the data and personnel capacity to adequately develop SMA capabilities for planning. Manning requirements and expertise are significant limitations for Army formations. The persistence and global scope required to identify normalcy and emergence is great. Researching the past like in the RAND study of Iranian elections is much more manageable. Knowing where to look and what to look for is a daunting task especially for a newly formed JTF. It appears the capability would need to be generating the data long before a JTF goes into planning mode. An existing system that JTFs and subordinate units plug into is a possible option.

CONCLUSION

The purpose of this monograph is to increase discourse on using advanced analytical processes applied to cyberspace for generating understanding of operational environments. The focus is blending relational systems in cyberspace with the military land domain. “How does the Army at corps level JTFs and below leverage cognitive information from cyberspace to create a more complete understanding of operational environments?” Analysis of contemporary Joint and Army doctrine, “what we do” points to a gap. The gap is a lack of discourse on the utility and cross-functional applicability of cognitive information gained from cyberspace. Doctrine has no answers for the unfamiliar application of a tool across dual domains and multiple functional area disciplines for environmental framing. Examination of SMA applied to the Haitian and Iranian cases provides evidence supporting two ideas. First, corps level and below echelons need persistent access to capabilities like SMA to frame environments and identify emergence in systems. Second, SMA as a capability can produce strategic level actionable understanding with population based tactical significance.

This monograph addressed the viability of SMA as an enabling capability for operational and tactical echelons. How to implement this capability will require an iterative process of Army organizational growth and adaptation. A likely approach is to develop a persistent capability for monitoring, and archiving the cyberspace environment by regions, led by the NSA, as the national agency tasked with visibility of this type of data. The Joint Staff or Geographic Combatant Commanders (GCC) could then establish enduring relationships with the NSA,

USCYBERCOM, or service cyber commands for regionally aligned teams.[83] These teams would retain authorities to monitor template geographic regions permanently, becoming regional experts or librarians. They would use the SMA capability just as the business and national intelligence communities do to paint a persistent near real time picture of the their environments using predominantly open sources of information. As JTFs or CJTFs are formed, cyber experts from a notional, regionally aligned Joint Interagency Cyber Team (JIACT) could then be assigned to the JTF Commander from their permanent position within the Joint Staff or GCCs.[84] When teams are tied to a Joint Staff regional board or GCC, organizational incentive exists to maintain a pulse on regional indicators and identify emergence. The JTF Commander then becomes directly

---

[83] U.S. Joint Chiefs of Staff, Joint Publication (JP) 1-0, *Doctrine of the Armed Forces of the United States.* Washington, DC: Government Printing Office, 2009, xiv. Defining a GCC; "The Commanders, US Central Command, US European Command, US Pacific Command, US Southern Command, and US Northern Command are each assigned a geographic area of responsibility (AOR) within which their missions are accomplished with assigned and/or attached forces. Forces under the direction of the President or the SecDef may conduct operations from or within any geographic area as required for accomplishing assigned tasks, as mutually agreed by the CDRs concerned or as specifically directed by the President or the SecDef. Functional CCDRs support geographic combatant commanders (GCCs), conduct operations in direct support of the President or the SecDef normally in coordination with the GCC in whose AOR the operation will be conducted, and may be designated by the SecDef as the supported CCDR for an operation."

[84]U.S. Joint Chiefs of Staff, JP 1-0, *Doctrine of the Armed Forces of the United States*, xxii. The notional JIACT organization could fall within the existing Joint Interagency Coordination Group. "When formed, a joint interagency coordination group (JIACG) can provide the CCDR with an increased capability to collaborate with other USG civilian agencies and departments. The JIACG, an element of a GCC's staff, is an interagency staff group that establishes and enhances regular, timely, and collaborative working relationships between other governmental agencies' representatives and military operational planners at the combatant commands. If augmented with other partners such as IGOs, NGOs, and/or multinational representatives, the JIACG enhances the capability to collaborate and coordinate with the private sector and/or regional organizations."

supported by the interagency elements that retain title authorities for the environments. Thus he controls his portion of the interconnected cyberspace operational environment. The JIACT would need to provide enough personnel to fulfill subordinate unit requirements possibly down to the Brigade level.

This preliminary organizational logic provides a framework that maximizes the persistent management of data and meets the subordinate unit personnel requirement for plugging into the library of cyber information. Additionally within JTFs, commanders two and three levels down could retain, on their staffs, the technical expertise for planning operational and tactical echelon approaches to solving increasingly more complex dual domain problem-sets. To codify this notion the following scenario provides a blended approach of the application of SMA as a tool for generating understanding through cyberspace.

Scenario Application

In 2013 AFRICOM establishes a corps size Combined Joint Task Force (CJTF) for deployment into the North West region of Africa to: stop atrocities; conduct regime change in country X; and stabilize the region. United States ground strength is capped at 11,000 personnel. CENTCOM continues as the overall supported GCC because of political and military attention pertaining to issues in Syria, a war in Afghanistan, and heightened tensions with Iran. The American CJTF Commander pulls in his planning team and initiates the Army design process to develop an operational approach for executing this economy of force mission. Without a history of U.S. entry into the region the environment is characterized as unfamiliar. There are geo-strategic implications with India, China, and European nations over access and legitimacy. Problem-sets are likely unprecedented for the CJTF. The Commander wants to leverage cyberspace information to generate greater shared understanding of the environment for the development of options. The Commander views the social layer of cyberspace as a vehicle for

reinforcing measures of performance and effectiveness for long duration campaigns. This is because of social media and cyberspace observed influence during the Arab-Spring. Prior to entry into the environment comprehensive understanding of the cyberspace domain becomes critical for the judicious application of resources.

Focus for the planning team is not the kinetic reduction of a conventional military system. The focus must be to understand relations between regional and local actors, populations at multiple scales, and influences. Currently the CJTF planning team must figure out who owns the analysis of this information from cyberspace. Does it belong to Information Operations, Signals intelligence, OSINT, Cyber Command, Army Cyber, contracted, or National assets? Where does the team go to gain this understanding? And how can the team retain the capability to monitor all these relationships over an extended period of time to identify emergence and measures of effectiveness?

Because this process requires persistent data archiving, trending, and infrastructure the team needs a reach back mechanism to an organization adapted to the investigation of the social layer of cyberspace and able to anticipate requirements. Enter in the JIACT (theoretical cyberspace support element), now the CJTF and subordinate BCTs retain a mechanism to plug-in to existing synthesized data from a joint organization that can circumvent service and agency parochialisms. In function this might look like a version of the online Open Source Center with technical experts managing the flow of information from the United States. Thus, the distributed

personnel requirement might be a single JIACT operator for any given operational or tactical echelon.[85]

The planning team begins designing two environments assisted by the JIACT. These environments are the physical military domains, and a separate aggregated virtual environment from cyberspace. The cyberspace COP is socialized across the breadth and depth of the CJTF planning staff. Coalition partners, multinational corporations, nongovernmental agencies and all applicable niche discipline functional areas collaborate on the process. They blend the two environments mixing anthropological research and existing understandings with dynamic systems relations extracted from the social layer of cyberspace building on near real-time models of DIME, PMESII-PT, ASCOPE and METT-TC. The product leads to a more adaptable operational approach with greater clarity of the population clusters and governmental control systems. Additionally, framing two environments provides the commander with a cognitive dimensional baseline of the Joint Operations Area and Area of Interest (the separate cyberspace environment). This baseline aids in the development of Measures of Effectiveness (MOE) and Measures of Performance (MOP) for the operational approach. Cyberspace trending points to emergence that feeds the MOEs and MOPs. The early identification of emergence and correlations with symbols,

[85]The Open Source Center provides online access to pertinent security related open source intelligence; military personnel of any discipline or background can readily access information an analogy is the early bird for INTEL. For further inquiry reference the Open Source Center website at https://www.opensource.gov (accessed 27 March 2013).

rituals, artifacts, and behaviors gives the commander an opportunity for adapting his approach and indicators of the necessity to reframe. [86]

This scenario shows utility of concept. The gap analysis and approach of this monograph provide evidence to the viability of SMA as a tool for increasing shared understanding within operational echelons for dual domain environmental framing. The capability fulfills a requirement using open sources of data enabling a high degree of distribution. The adaptive nature of the tool provides cross-functional utility and collaboration.

Recommendation for Further Research and Doctrine

Recommended areas for further research include the proliferation of this capability outside of the United States DOD and IC to ask questions like; What countries or who is using this stuff, and doing it well? Does the United Sates possess asymmetry in cyberspace environmental understanding? If so, how long will it last? Who are the major corporations selling their products to? All of these questions need answers in order to fuel discourse on government policy, public perception, and secrecy issues.

Recommendations for Army doctrine are three fold. First, generate a discourse on the cross-functional application of SMA and similar tools for blending understanding of the social layer of cyberspace across multiple domains. Key documents for this discourse are ADRP 3-0, and 5-0, because these are the documents that commanders and planners know, and these

[86]Department of the Army, ADRP 5-0, *The Operations Process*, 2-11. "Reframing is the activity of revisiting earlier design hypotheses, conclusions, and decisions that underpin the current operational approach. In essence, reframing reviews what the commander and staff believe they understand about the operational environment, the problem, and the desired end state."

documents feed joint doctrine. Second, train leaders on cyberspace and the resources that can be plugged into or requested. Cyberspace is power, leaders at all levels must know how to harness the opportunities and understand the domain. The final recommendation is to produce a discourse on how to organize for the cyberspace domain. It is not enough to simply develop an additional functional area or hand this to an overloaded discipline such as INTEL or IO. Operational Commanders must exert control over these cyberspace capabilities. Unnecessary risk to the mission and force could occur if domain responsibility becomes diffused among sub-unified commands and separate agencies.

This monograph used existing concepts, rearranged them and focused on understanding environments through the cognitive dimension of the social layer. In the end, the ability to reduce an adversarial system and defend our own only provides flexibility; understanding, creates adaptability. This understanding is needed most in the Army and Joint echelons that enter adversarial and neutral systems. Those forces will change the preferences, sentiments, intentions, and interests of populations for decades to come.

BIBLIOGRAPHY

Primary sources

Alexander, Keith B., General. Commander United States Cyber Command. Statement Before the Senate Committee on Armed Services, 27 March 2012.

Chen, Hsinchun. *Intelligence and Security Informatics for International Security: Information Sharing and Data Mining (integrated Series in Information Systems)*. New York: Springer, 2009.

Chen, Hsinchun, Roger H. L. Chiang, and Veda C. Storey. "Business Intelligence and Analytics: From Big Data to Big Impact." *MIS Quarterly* 36, no. 4 (December 2012): 1165-1188.

Chairman, Joint Chiefs of Staff. Joint Publication (JP) 1, *Doctrine of the Armed Forces of the United States.* Washington, DC: Government Printing Office, 2009.

_____. Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations.* Washington, DC: Government Printing Office, 2012

_____. Joint Publication (JP) 3-13, *Information Operations.* Washington, DC: Government Printing Office, 2012.

_____. Joint Publication (JP) 6-0, *Joint Communications System.* Washington, DC: Government Printing Office, 2010.

_____. Joint Publication (JP) 6-01, *Joint Electromagnetic Spectrum Management Operations.* Washington, DC: Government Printing Office, 2012.

Clapper, James R. *Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record; for Senate Select Committee on Intelligence*. Washington, DC: Office of the Director of National Intelligence, 12 March 2013.

Defense Advanced Research Projects Agency (DARPA). *Broad Agency Announcement XDATA: DARPA-BAA-12-38*. Arlington, VA: Information Innovation Office (I2O), 29 March 2012.

Dempsey, Martin E. *Joint Information Environment White Paper 22 January 2013*. Washington, DC: Government Printing Office, 2013.

Department of the Army. *Army Strategic Planning Guidance*. Washington, DC: Government Printing Office, 2013.

_____. Army Doctrine Publication (ADP) 3-0, *Unified Land Operations*. Washington DC: Government Printing Office, 2011.

_____. Army Doctrine Publication (ADP) 5-0, *The Operations Process*. Washington DC: Government Printing Office, 2012.

_____. Army Doctrine Publication (ADP) 6-0, *Mission Command.* Washington DC: Government Printing Office, 2012.

_____. Army Doctrine Reference Publication (ADRP) 2-0, *Intelligence*. Washington DC: Government Printing Office, 2012.

_____. Army Doctrine Reference Publication (ADRP) 3-0, *Unified Land Operations*. Washington DC: Government Printing Office, 2012.

_____. Army Doctrine Reference Publication (ADRP) 5-0, *The Operations Process.* Washington DC: Government Printing Office, 2012.

_____. Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command.* Washington DC: Government Printing Office, 2012.

_____. Field Manual (FM) 3-13, *Inform and Influence Activities.* Washington, DC: Government Printing Office, 2013.

_____. Field Manual (FM) 3-36, *Electronic Warfare*. Washington, DC: Government Printing Office, 2012.

_____. Field Manual (FM) 3-38, *Cyber Electromagnetic Activities.* Washington, DC: Government Printing Office, 2013.

_____. Field Manual (FM) 3-55, *Information Collection.* Washington, DC: Government Printing Office, 2012.

_____. Field Manual (FM) 5-0, *The Operations Process.* Washington, DC: Government Printing Office, 2010.

_____. TRADOC Pamphlet 525-7-8, *Cyberspace Operations Concept Capability Plan 2016-2028.* Washington DC: Government Printing Office, 2010.

Department of Defense. *Strategy for Operating in Cyberspace*. Washington, DC: Government Printing Office, 2011.

Dugdale, Julie, Bartel Van De Walle, and Corinna Koeppinghoff. "Social Media and SMS in the Haiti Earthquake." *WWW 2012 Companion* (16-20 April 2012): 713-714.

NSF 12-499. Program Solicitation. "Core Techniques and Technologies for Advancing Big Data Science." *National Science Foundation* (1 October 2010).

Office of Science and Technology Policy Executive Office of the President. *Obama Administration Unveils "big Data" Initiative*. Washington, DC: Office of Science and Technology Policy Executive Office of the President, 2012.

Office of the Director of National Intelligence. *Global Trends 2030: Alternative Worlds*. Washington DC: National Intelligence Council, 2013.

Pool, Robert, Rapporteur. *Sociocultural Data to Accomplish Department of Defense Missions*. Workshop Summary. Washington, DC: National Academy of Sciences, 2011.

Porche, Isaac R. III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, and Bruce J. Held. *Redefining Information Warfare Boundaries for an Army in a Wireless World.* Santa Monica, CA: RAND Corporation, 2013.

Truvé, Staffan. "Big Data for the Future: Unlocking the Predictive Power of the Web." *Recorded Future,* Cambridge, MA (2011).

_____. "A White Paper on Temporal Analytics." *Recorded Future* (2010).

White House. “Obama Administration Unveils ‘Big Data’ Initiative: Announces $200 Million in New R&D Investments.” *Office of Science and Technology Policy*. Washington, DC: Government Printing Office, 2012.

Yates, Dave, and Scott Paquette. “Emergency Knowledge Management and Social Media Technologies: A Case Study of the 2010 Haitian Earthquake.” *International Journal of Information Management* 31 (2011): 6-13.

Yeung, Douglas, Parisa Roshan, S. R. Bohandy, and Alireza Nader. *Using Social Media to Gauge Iranian Public Opinion and Mood after the 2009 Election*. RAND National Security Research Division, 2012.

Secondary sources

Abouzeid, Rania. “Bouazizi: The Man Who Set Himself and Tunisia on Fire.” *Time* (21 January 2011). http://www.time.com/time/magazine/article/0/9171/2044723.00.html (accessed 23 September 2013).

Chen, Hsinchun. “Artificial Intelligence Laboratory: Intelligence and Security Informatics,” *University of Arizona Eller College of Management*. http://ai.arizona.edu/ research/isi/ (accessed 4 June 2013).

Cooper, Adam. “A Brief History of Analytics.” *JISC CETIS* 1, no 9 (2012).

Computer Science and Telecommunications Board. *Public Response to Alerts and Warning Using Social Media*. Workshop Report. Washington, DC: National Academy of Sciences, 2013.

Cone, Robert W., General. “Laying the Groundwork for the Army 2020.” *Land Warfare Publication* 11-2 (August 2011): 1-3.

Cukier, Kenneth, and Viktor Mayer-Schoenberger. “The Rise of Big Data: How It’s Changing the Way we Think About the World.” *Foreign Affairs* (May/June 2013).

IBM. *Social Media Analytics: Making Customer Insights Actionable.* Somers, NY: IBM Corporation, 2013.

Kaplan, Andreas M., and Michael Haenlein. “Users of the World, Unite! The Challenges and Opportunities of Social Media.” *Business Horizons* 53, no. 1 (2011): 59-68.

Marin, Alexandra, and Barry Wellman. “Social network analysis: An introduction.” *Sage Handbook of Social Network Analysis.* London (2011): 11-25.

Melville, Prem, Vikas Sindhwani, and Richard D. Lawrence. “Social Media Analytics: Channeling the Power of the Blogosphere for Marketing Insight.” *CiteSeer* (2009).

Odierno, Ray, GEN. “The Force of Tomorrow.” *Foreign Policy* (4 February 2013). http//www.foreignpolicy.com/articles/2013/02/04/the_force_of_tomorrow (accessed 2 October 2013).

U.S. Strategic Command. “U.S. Cyber Command Mission Statement.” *USCYBERCOM*. http://www.arcyber.army.mil/org-uscc.html (accessed 12 July 2013).

Additional works consultedFisher, Bill, and Hayley Miller. “Social Media Analytics, How It Can Help Shape Government Performance.” *MicoTech/White Papers* (December 2011).

Horvitz, Eric, and Tom Mitchell. “From Data to Knowledge to Action: A Global Enabler for the 21st Century.” *Computing Community Consortium* (27 June 2010).

Johansson, Fredrik, Joel Bynielsson, Pontus Horling, Michael Malm, and Christian Martenson. *Detecting Emergent Conflicts through Web Mining and Visualization*. Stockholm, Sweden: Swedish Defence Research Agency, 2011.

Raytheon Company. “Raytheon Leads Efforts to Build a Scalable, Interoperable Analytics System to Aid Defense.” *PRNewswire* via COMTEX, Linthicum, MD, 9 June 2010.

Samaan, Jean-Loup. “Cyber Command: The Rift in US Military Cyber-Strategy.” *The RUSI Journal* 155, no. 6 (2010): 16-21. http://dx.doi.org/10.1080/03071847.2010.542664 (accessed 11 February 2013).

SAS. “Integrate, Archive, Analyze and Act on Online Conversations.” *SAS The Power to Know.* SAS Institute Inc. World Headquarters.

Stelzner, Michael A. *How Marketers are Using Social Media to Grow Their Businesses*. Social Media Marketing Industry Report, 2011.